(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平4－252350

(43)公開日　平成４年(1992)９月８日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	15/00	３３０　Ｄ	7323－5L		
	12/14	３２０　Ａ	8841－5B		
	15/16	４７０　Ｍ	9190－5L		

審査請求　未請求　請求項の数１(全　４　頁)

(21)出願番号　特願平3－8299

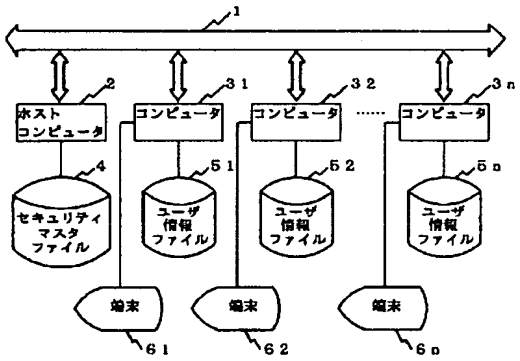
(22)出願日　平成３年(1991)１月28日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　小田島　孝
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア工場内
(72)発明者　織茂　昌之
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　平澤　茂樹
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　セキュリテイチエツク方法

(57)【要約】
【目的】不正利用者の積極的な発見のためのセキュリティチェック方法を提供すること。
【構成】コンピュータ３１は、端末６１から入力されたユーザＩＤ７とパスワード８に、コンピュータ３１の持つ端末ＩＤ９を附加してセキュリティを強化した上でホストコンピュータ２へ送信する。受信したホストコンピュータ２は、予め登録されたユーザＩＤ７とパスワード８と端末ＩＤ９と、受信したユーザＩＤ７とパスワード８と端末ＩＤ９とを比較する。ホスト側コンピュータは、端末６１から入力されたユーザＩＤ７とパスワード８は一致するが、コンピュータ３１が附加した端末ＩＤ９が一致しない場合、不正利用者として、予め指定した範囲のアクセスを許可し、使用を継続させ、その間に不正利用者の調査を行う。

本発明の一実施例のネットワークシステムの構成図（図１）



1

【特許請求の範囲】

【請求項１】第１のセキュリティ情報を有する第１のコンピュータと、第２のセキュリティ情報を有する第２のコンピュータを有するコンピュータシステムにおいて、該第２のコンピュータは、該第２のコンピュータに入力された第３のセキュリティ情報に該第２のコンピュータが持つ該第２のセキュリティ情報を附加して該第１のコンピュータに送信し、該第１のコンピュータは、受信した該第２、第３のセキュリティ情報と該第１のコンピュータが有する該第１のセキュリティ情報とを比較し、該第３のセキュリティ情報は一致するが、該第２のセキュリティ情報が一致しない場合に、予め指定された範囲のアクセスを許可することを特徴とするセキュリティチェック方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】セキュリティのチェック方法に関する。

【０００２】

【従来の技術】従来の方法は、特開平２－２０８７７０号公報に記載のように、セキュリティチェックを強化することにより不正な侵入を防止していた。

【０００３】

【発明が解決しようとする課題】上記従来技術では、不正な利用者を防止することを目的としており、不正利用者を発見する点での配慮がされておらず、不正利用者が突き止められないという問題があった。

【０００４】本発明の目的は、不正利用者の積極的な発見のためのセキュリティチェック方法を提供することにある。

【０００５】

【課題を解決するための手段】上記目的を達成するために、第２のコンピュータへ入力される第３のセキュリティ情報に、第２のコンピュータの持つ第２のセキュリティ情報を附加してセキュリティを強化した上で第１のコンピュータへ送信する。第１のコンピュータは、予め登録された第１のセキュリティ情報と受信した第２、第３のセキュリティ情報を比較する。第１のコンピュータは、第２のコンピュータへ入力された第３のセキュリティ情報は一致するが、第２のコンピュータが附加した第２のセキュリティ情報が不一致の場合は、不正利用者の通知を行い、不正利用者として予め指定した範囲でのアクセスを許可し、使用を継続させ、その間に不正利用者の調査を行う。

【０００６】

【作用】セション開始時のチェックは、第２のコンピュータへ入力された第３のセキュリティ情報と第２のコンピュータが附加する第２のセキュリティ情報が、第１のコンピュータに送信され、第１のコンピュータに登録された第１のセキュリティ情報と一致するか否かが確認される。第２のコンピュータへ入力された第３のセキュリティ情報は一致するが、第２のコンピュータが附加した第２のセキュリティ情報が不一致の場合でも、利用者に対しては接続を許可し、使用を継続させて調査する時間をつくると共に、第１のコンピュータは警告を発する。

【０００７】

【実施例】以下、本発明の一実施例を図面により詳細に説明する。図１は本発明の一実施例のネットワークシステムの構成図である。ネットワークシステムはネットワーク１により結合されたホストコンピュータ２と複数のコンピュータ３１，３２，…３ｎからなる。ホストコンピュータ２はセキュリティマスタファイル４を有する。コンピュータ３１，３２，…３ｎはユーザ情報ファイル５１，５２，…５ｎと、端末６１，６２，…６ｎを有する。

【０００８】図２は、セキュリティマスタファイル４とユーザ情報ファイル５１，５２，…５ｎのセキュリティ情報１０のデータ構成図である。セキュリティ情報１０はユーザＩＤ７とパスワード８と端末ＩＤ９からなる。

【０００９】本実施例では、セキュリティ情報１０が二重化されている。ホストコンピュータ２のセキュリティマスタファイル４には、予め、ネットワークシステムの全ユーザのユーザＩＤ７と、それに対応するパスワード８と端末ＩＤ９が登録されている。端末側コンピュータのユーザ情報ファイル５１，５２，…５ｎには、各ユーザ毎のユーザＩＤ７と、それに対応するパスワード８と端末ＩＤ９が登録されている。ユーザ情報ファイル５１，５２，…５ｎには、同じユーザＩＤ７は登録されない。

【００１０】図３は処理の手順を示すフローチャートである。セション開始時に、利用者がコンピュータ３１に接続される端末６１から、ユーザＩＤ７とパスワード８を入力する（ステップ１１）。コンピュータ３１内のユーザ情報ファイル５１がユーザＩＤ７をキーに検索される（ステップ１２）。検索できたか否かを判断する（ステップ１３）。検索できた場合は、検索の結果得たユーザ情報ファイル５１内のパスワード８と、利用者が入力したパスワード８を比較する（ステップ１４）。パスワード８が一致したら、ユーザＩＤ７とパスワード８と端末ＩＤ９からなるセキュリティ情報１０をホストコンピュータ２へ送信し、セション開始要求を行う（ステップ１５）。ホストコンピュータ２からの応答を待つ（ステップ１６）。検索ができなかった場合、パスワード８が一致しなかった場合は、端末側コンピュータ３１はホストコンピュータ２を使用することはできない。

【００１１】ホストコンピュータ２はコンピュータ３１，３２…３ｎからのセション開始要求を待つ（ステップ２１）。ホストコンピュータ２はセション開始要求を受信したら、受信したユーザＩＤ７をキーにセキュリティマスタファイル４を検索する（ステップ２２）。検索

できたか否かを判断する（ステップ２３）。検索できなかった場合は、セキュリティ情報不正で送信する（ステップ２９）。この場合、コンピュータ３１は、セション開始許可情報でないので、セション開始できない（ステップ１７）。

【００１２】検索できた場合は、検索の結果得たパスワード８を受信したパスワード８と比較する（ステップ２４）。パスワード８が一致しない場合は、セキュリティ情報不正で送信する（ステップ２９）。この場合、コンピュータ３１は、セション開始できない（ステップ１７）。パスワード８が一致したら、受信した端末ＩＤ９と検索の結果得た端末ＩＤ９が、一致するかを判断する（ステップ２５）。端末ＩＤ９が一致したら、正当な利用者として、セション開始許可情報を送信する（ステップ２６）。端末側コンピュータ３１は受信した情報がセション開始許可情報か否かを判断する（ステップ１７）。セション開始許可情報であり、不正利用者ではないので（ステップ１８）、コンピュータ３１は、正当な利用者として、セションを開始する。

【００１３】ユーザ情報ファイル５１に他の端末側コンピュータ用のユーザＩＤ７とパスワード８を登録した場合等、パスワード８は一致するが端末ＩＤ９が一致しない場合は、まず、ホストコンピュータを管理している者に対して、不正利用者が存在することを通知する（ステップ２７）。次に、不正利用者用として予め指定した範囲のアクセス許可をもたせて、セション開始許可情報を送信する（ステップ２８）。端末側コンピュータ３１は受信した情報がセション開始情報か否かを判断する（ステップ１７）。セション開始許可情報であるが、不正利用者なので（ステップ１８）、コンピュータ３１は、セションを開始できるが、アクセスできる範囲は、不正利用者用に予め指定された範囲に限られる。このように、不正利用者に使用を継続させて調査する時間をつくり、不正利用者の調査を行う。不正利用者は、正規のユーザＩＤ７とパスワード８を入力したので、正規にアクセスできたと思いこむ可能性がある。

【００１４】なお、予め指定した範囲のアクセスとは、例えば、見られても実害のないファイルを予めホストコンピュータ２の管理者が指定してその部分のデータを参照させるとか、不正利用者用のダミーのファイルを設けて、そのファイルにのみアクセスを認める等ということである。

【００１５】本実施例では、セキュリティ情報１０が二重化されており、端末側コンピュータ３１，３２…３ｎにおいても、ユーザＩＤ７をキーにパスワード８を検索し、一致するか否かをチェックしている。また、端末側コンピュータ３１，３２…３ｎが附加する端末ＩＤ９は、端末側コンピュータ３１，３２，…３ｎ毎に対応しておらず、ユーザＩＤ７毎に対応している。また、端末ＩＤ９は変化しない。

【００１６】しかし、入力されたユーザＩＤ７とパスワード８を端末側コンピュータ３１，３２…３ｎでチェックしなくとも良い。また、端末ＩＤ９は端末側コンピュータ３１，３２…３ｎ毎に対応させ、端末側コンピュータ３１，３２，…３ｎ毎に有する端末ＩＤ９を、入力されたユーザＩＤ７とパスワード８に附加することにしても良い。また、端末側コンピュータ３１，３２，…３ｎが付加する端末ＩＤ９を可変にしても良い。

【００１７】また、本実施例は、端末側コンピュータ３１，３２，…３ｎとホストコンピュータ２から構成されている。しかし、分散型データベースのように、すべてのコンピュータがホストと端末両方の役割を果たすようにしても良い。その場合には、各コンピュータが、自コンピュータにアクセス可能なユーザＩＤ７等を登録したファイルを持てば良い。そして、不正利用者がある場合、アクセスされたコンピュータを管理するものに対して、不正利用者の存在することを通知する。

【００１８】また、本実施例では、入力されたユーザＩＤ７とパスワード８と端末側コンピュータ３１，３２，…３ｎが附加した端末ＩＤ９が加工されていない。つまり、端末側から送信されたユーザＩＤ７とパスワード８と端末ＩＤ９と、ホストコンピュータ２が有するユーザＩＤ７とパスワード８と端末ＩＤ９は同じものである。しかし、ホストコンピュータ２が、予め登録された一定の規則に従って、受信したセキュリティ情報１０を加工し、その加工した結果とホストコンピュータ２が有するセキュリティ情報１０を比較することにしても良い。また、端末側コンピュータ３１，３２，…３ｎが入力されたユーザＩＤ７とパスワード８を加工して、送信しても良い。

【００１９】本実施例によれば、正規の端末であるコンピュータ３２に接続された端末６２から他の端末側コンピュータ用のユーザＩＤ７とパスワード８を調べてセションを開始しようとした場合、コンピュータ３２にあるユーザ情報ファイル５２にユーザＩＤ７とパスワード８が登録されていないために、ユーザ情報ファイル５２を検索した時点でエラーとなり、ユーザ間でのパスワードの盗用が防止できるという効果がある。

【００２０】

【発明の効果】本発明によれば、利用者が入力するセキュリティ情報は一致するが、入力側コンピュータが附加したセキュリティ情報が不一致の場合でも、その不正利用者に対して予め指定された範囲のアクセスを許可し、使用を継続させ、受信側には不正利用者の通知を行い、不正利用者の調査を行うことにより不正利用者の発見が容易であるという効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例のネットワークシステムの構成図である。

【図２】セキュリティマスタファイルとユーザ情報ファ

5

イル内のセキュリティ情報のデータフォーマットを示す図である。

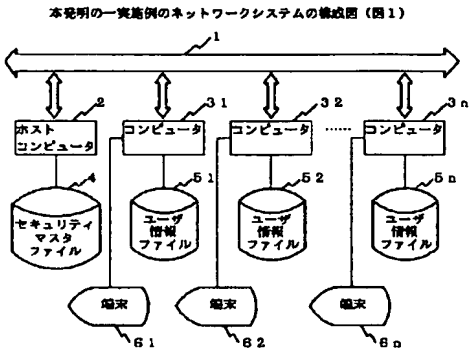
【図３】処理手順を示すフローチャートである。

【符号の説明】

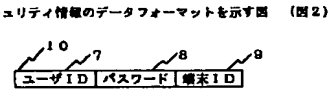
１…ネットワーク、２…ホストコンピュータ、３１，３２～３ｎ…コンピュータ、４…セキュリティマスタファイル、５１，５２～５ｎ…ユーザ情報ファイル、６１，６２～６ｎ…端末、７…ユーザＩＤ、８…パスワード、９…端末ＩＤ、１０…セキュリティ情報。

6

【図１】



【図２】



【図３】